Version 3.1 October 2020

# China CITIC Bank
# London Branch

# Risk Management Framework

中信银行 CHINA CITIC BANK 伦敦分行 LONDON BRANCH

**Document History**

| | | | |
|---|---|---|---|
| **Author** | Chief Risk Officer | **Status** | FINAL |
| **Version** | 3.1 | **Date** | 26/11/202 |
| **Approved by** | ARCo | | |
| **Location** | London | **Next Review Date** | October 2021 |

| Version | Owner | Approval | Date | Major changes |
|---|---|---|---|---|
| 1.0 | President | President | May 2018 | PRA Regulatory Business Plan |
| 1.1 | CRO | MANCO | Sept 2018 | As per approval dated 24/10/2018 |
| 2.1 | CRO | MANCO | Oct 2019 | As per approval dated 25/10/2019 |
| 3.1 | CRO | ARCO | Nov 2020 | • Approval – changed to ARCo (8)<br>• Liquidity Risk – align with ALCO decision and Liquidity Risk Policy (13)<br>• Three LOD – change FM responsibilities around Liquidity risk to align with above point (17)<br>• Terms of references – attached separately<br>o Appendix C – Management Committee<br>o Appendix D – Asset & Liability Committee<br>o Appendix E – Audit & Risk Committee<br>o Appendix F – Credit Committee |

## CONTENTS

## 1 Introduction

This document is an integral part of the overall risk management framework established by China CITIC Bank London Branch ("CNCBLB" and / or "the Branch") and must be read in conjunction with the Risk Appetite Statement ("RAS") and other risk management policies.

The Risk Management Framework ("RMF") sets out the process by which the senior management at CNCBLB will operate within the delegated authority of China CITIC Bank Head Office ("CNCB" or "HO") and the UK regulations set by the Prudential Regulation Authority ("PRA") and the Financial Conduct Authority ("FCA"), together referred to as "the UK regulators".

The regulators pursue objectives to promote the safety and soundness of regulated firms, thereby promoting stability of the financial system, and to ensure relevant markets function effectively. Operationally, its objectives for properly functioning markets are to ensure an appropriate degree of protection for consumers, protect and enhance the integrity of the financial system and promote effective competition in the interests of consumers. CNBCLB is authorised by the PRA and regulated by both the FCA and the PRA.

The UK regulators expects firms to have in place clear structures of accountability and delegation of responsibilities for individuals and committees, including checks and balances to prevent dominance by an individual. Senior individuals should remain accountable for the actions of those to whom they delegate responsibilities, including use of third parties in respect of outsourced functions.

The regulator authorises firms to conduct regulated activities and, in those firms, authorises individuals who perform controlled functions, which are roles that have a particular regulatory significance and are Senior Management functions ("SMF") – see ***Appendix A*** for CNCBLB approved SMF's

These appointments carry personal accountability to the regulator and are responsible for ensuring that the firm is managed prudently. In furtherance of this, each senior manager is appointed to one or more senior manager functions, which have inherent responsibilities, as well as a set of prescribed obligations and a statement setting out those areas of overall responsibility. This information forms part of the application to the regulators for appointing individuals who hold SMFs, making clear individual accountability. The expectation of these individuals is to meet standards of professional conduct that are as exacting to those expected of firms by the UK regulators. To make clear its expectations of personal conduct, the regulator has established a code of conduct,

comprising five conduct rules for all staff members and a further set of four rules for those who holds SMFs (See ***Appendix B*** - Principles & Conduct rules).

UK regulatory expectations of firms, generally, for prudential and conduct matters, are published by the regulators in a collection (Handbook) of sourcebooks, covering the range of financial activities carried out in the UK. The purpose of the sourcebook called Senior Management Arrangements, Systems and Controls (SYSC) is to promote effective governance control in firms, expressed thus:

1. to encourage firms' senior managers to take appropriate practical responsibility for their firms' arrangements on matters likely to be of interest to the appropriate regulator because they impinge on appropriate regulator's functions under the Act (Financial Services & Markets Act 2000);
2. to increase certainty by amplifying Principle 3, under which a firm must "take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems";
3. to encourage firms to vest responsibility for effective and responsible organisation in specific senior managers; and
4. to create a common platform of organisational and systems and control requirements for all firms.

The structure of this document has been based on the contents of SYSC, having regard to the individual responsibilities and accountability bestowed upon those who hold senior management functions.

In order to manage risk, the Branch operates a three lines of defence ("TLOD") risk management framework through which risks are identified, assessed, monitored and controlled.

The RMF implemented by the Branch is similar to that used by Head Office ("HO"). Although the President will delegate authority for the detailed review and power of recommendation to the CNCBLB Audit and Risk Committee ("ARCo"), it is HO that is ultimately responsible for the Branch's risk framework.

## 2 Objectives

The objectives of the RMF are to:

- provide a concise and coherent description of the corporate governance and risk management framework established by the Branch's senior management;
- provide evidence that senior management have given due consideration to the allocation of management responsibilities in accordance with current regulatory requirements;
- provide an efficient method of conveying information on the subject of governance and risk management in CNCBLB to interested parties e.g. HO, employees, auditors, regulators etc.
- Outline the key risks arising from the planned business within the Branch and the associated mitigants implemented to manage these;
- Outline the RMF and the key component parts of which it comprises. The includes the roles of individual departments, the range of supporting policies and processes in place to ensure effective implementation of the framework, and the governance surrounding both the implementation of this document and the wider RMF; and
- Provide an overview of how the Branch seeks to identify and assess risk, including the Branch's risk scoring methodology.

## 3 Ownership

The ownership structure of this document has been set out below.

| | |
|---|---|
| **Framework Owner** | The Branch's Chief Risk Officer ("CRO") is responsible for the maintenance for this document.<br><br>The CRO will also be responsible for reviewing the framework document on an annual basis or more frequently as required.<br>Review outside the annual cycle could be triggered by:<br><br>• Change in CNCBLB's strategy;<br>• Change in the Branch's Control Framework;<br>• Change in the Regulatory requirements; and/or<br>• Change in HO's risk appetite and/or strategy.<br><br>Any material changes to this document will be communicated to staff accordingly. |
| **Challenge** | Following review by the CRO, the Audit and Risk Committee ("ARCo") will review and challenge this framework document. Again, this must occur at least annually or more frequently as required.<br><br>The approval or otherwise must be presented to the Management Committee ("ManCo") following each review. |
| **Approval** | ARCo, is responsible for final challenge and approval of this document. |
| **Applicability** | All members of staff, whether permanent (local hires and expatriate alike) or contractors must adhere to this policy.<br><br>Escalation of any matters arising in respect of this should be via the individual's Head of Department or directly to the CRO. |

# 4 Governance

This section sets out the arrangements for the governance of the Branch's RMF, including key committees, management structure and reporting lines.

## 4.1 Overview

As per the delegated authority from HO, the President of the Branch will have overall responsibility for the oversight and implementation of the framework. In order to have sufficient oversight of the RMF and its implementation, the President has delegated the day-to-day oversight responsibilities to the CRO, the Risk department and the Heads of the Branch's business lines.

The ARCo will also undertake detailed reviews, challenge the design and effectiveness of the framework and consider detailed information about the risk profile of the Branch. As part of its review and challenge, the ARCo will assess whether the RMF is fit for purpose and complies with local regulatory requirements.

## 4.2 Delegation of Authority by Head Office

The President will act under a formal Delegation of Authority ("DOA") from HO and will be empowered to make decisions, require changes to local policies and to sub-delegate aspects of his DOA to committees and individuals.

The Branch is required, where ever possible and feasible in the local jurisdiction, to follow all HO policies including China CITIC Bank credit, market, liquidity, and operational risk policies. Where such policies are not consistent with UK regulatory or legal requirements, the President will liaise with HO in order to augment HO policies as necessary to ensure that CNCBLB complies with its local regulatory requirements at all times.

Branch specific policies have been created to ensure alignment with UK regulatory requirements and to support the local implantation of the RMF (see Section 8 for a list of such local policies).

## 4.3 Head Office Oversight

CNCBLB as an extension of HO will naturally operate within the strategy and risk appetite of the Bank. The activities to be undertaken and the control arrangements to be implemented locally will reflect UK regulatory requirements to ensure ongoing compliance with all relevant regulatory requirements and expectations.

HO intends to effect oversight of CNCBLB through a range of different activities and direct touch-points. These include, but are not limited to:

- **Functional matrix reporting lines:** In addition to the local reporting lines into the Branch's senior management team, all Heads of department also have 'dotted' reporting lines into their corresponding HO function. Through this UK departmental Heads will maintain a personal bilateral engagement with HO and direct functional oversight can be implemented by HO;
- **Head Office Delegation of Authority:** HO will provide a formal DOA to the President. This will form the basis for all delegation of authority to other members of the senior management team as well as ManCo and the committees supporting ManCo. The DOA very importantly will also form the basis of the Branch RAS;
- **International Business Committee:** Committee set up specifically to act as the coordinator and escalation point for all matters relating to the London Branch (and other overseas entities in due course once established). This committee will be chaired by the HO VP in charge of overseas entities;
- **Reporting:** Supporting the bilateral dotted functional reporting lines, functional MI is provided on a quarterly basis from each department directly to the equivalent HO department. This will provide further line of sight from HO as well as ensure CBRC reporting requirements are met. Branch-wide performance related reporting will also be provided from the President to the VP at HO; and
- **Internal Audit arrangements:** HO's Internal Audit function will conduct audits as per their annual audit plan in respect of CNCBLB. These audits will be carried out to ascertain the extent to which HO requirements on the Branch are adhered to and to ensure that HO's own audit plan is completed in accordance with expectations to HO's Third Line of Defence.

### 4.4 Risk Appetite

In establishing the Branch RAS, all key risks were initially assessed using the Risk Scoring Methodology and captured in the Risk Matrix, as defined in the Operational Risk Policy. These identified risks were calibrated to risk appetite levels and commercial performance goals through the setting of broad measures for the Branch's risk appetite.

The Branch's risk appetite is set within the framework of HO's risk appetite and its relevant requirements. The London Branch will monitor its risk-specific bottom line and tolerance based on its positioning and bank-wide risk management requirements, and execute them in the business' risk management processes.

The Branch's RAS which is derived from the President's DOA is designed to:

- Be reflective of the Branch's strategy, including its organisational objectives, business plans, financial constraints and stakeholder expectations;
- Consider all key risks of the business;
- Be consistent with the CNCB risk appetite;
- Reflective of the willingness and capacity of the Branch to take on risk;
- Be encompassing in terms of the skills, resources and technology required to manage and monitor risk exposures in the context of the risk appetite;
- Include a defined tolerance for loss or negative events that can be reasonably quantified;
- Be reviewed annually in line with the Branch's business plan and whenever there is a material change to the business; and
- Be documented in a formal statement that is approved by the senior management.

The Branch RAS is developed in four formal stages:

- Determine the Branch's organisational strategic objectives;
- Develop the Branch strategic business plan;
- Align the Branch's risk appetite to the strategic business plan by:
    - Identifying material risks the Branch is exposed to that may prevent it achieving its strategic objectives;
    - Establishing the risk-taking capacity of the Branch over the life of the plan;
    - Establishing the risk appetite for each of the material risks post-mitigation; and
- Formalise the Branch's risk appetite through approval by HO.

Some of the key risk categories and the associated approach adopted by the Branch for measuring risk and of setting of limits are outlined below:.

### 4.4.1 Credit Risk

Risk Appetite Low/Conservative - Investment grade only across product, geographies and industry with tenors out to 5 years

Credit risk is measured in terms of the total exposure CNCBLB may have when a counterparty/borrower/issuer defaults, if the default occurs at the worst possible time over the life of

the transaction. Specifically, the peak exposure takes account of the potential impact of movements in market risk factors on the exposure.

The measure takes account of collateral and security arrangements, netting arrangements and guarantees, where legal opinions have been obtained confirming that such arrangements are enforceable under the applicable legal jurisdictions. The measure does not take account of the probability of default. The details of the methodologies used are set out in the CNCBLB Credit Approval and Credit Risk Management Policy.

Key measures used to quantify credit risk include:

- Total exposure to individual counterparties/borrowers/issuers; and
- Aggregated exposure to groups, countries and industry sectors.

Limits are set by Credit Committee on total exposure to individual counterparties/borrowers/issuers and on aggregated exposure to groups, countries and industry sectors. These limits are divided across the type of product traded (Treasury, Banking, Clearing etc.) which are effectively equivalent to limits by business unit. Tenor limits are also set on the products traded with each counterparty.

Corporate counterparty credit ratings are obtained both from external sources and from the internal HO rating model. Both ratings, where available, are utilised for reporting, but the HO rating is used where a rating is required to determine policy. Where more than one external rating is available, the policy is to use either the lower rating if two ratings are available, or the lower of the two highest ratings if more than two are available.

### 4.4.2 Market Risk

Risk Appetite Low/Moderate– restricted products; Bond investments, FX spot for customers and FX / Interest Rate hedging of credit business

Market risk is quantified in terms of:

- The calculation of a Foreign Exchange (“FX”) risk is the sum of all assets and liabilities in currency, and the risk of translating those back to USD, so the risk as calculated is to preserve the USD value of the balance sheet
- A ‘gap’ approach to measure its Interest Rate Risk in Banking Book, (“IRRBB”) exposure. This is determined as the maximum net position of interest earning assets and interest paying liabilities utilising actual maturity or maturity for interest rollover whichever is earlier. In addition, sensitivity analysis will be conducted regularly by Risk to understand the impact on net interest income based

on PVBP (1 Basis Point movement on interest rate curve), Duration risk, CS01 (1 Basis Point movement in credit spreads) and a ±200 Basis Points ("bps") stress shift in the interest rate curve.

The methodologies used are set out in CNCBLB Market Risk Management Policy.

Limits are set by ManCo in the RAS on sensitivities to individual risk factors and certain stress tests. Limits are divided across business units. Limits are also set on the tenor of products.

### 4.4.3 Liquidity Risk

Risk Appetite Medium/Conservative – maintain levels of liquidity coverage in line with HO support and UK regulatory requirements.

Liquidity risk is quantified in terms of CNCBLB's sources of funding and considers the possibility that CNCBLB cannot raise funding from its normal sources, and to its cash inflows and outflows, to account for the risk that expected cash inflows may not occur or there may be unexpected draw-downs from committed facilities or under collateral arrangements.

Liquidity risk is measured in terms of:

- 30 day cumulative contractual mismatch; and
- Asset & Liability mismatch out to 5 years.

Furthermore, the UK regulator monitor liquidity risk through the Liquidity Coverage Ratio of the 'Total Bank' which is reported at least half yearly.

### 4.4.4 Operational Risks

Risk Appetite Medium/Moderate– inherent operational risk for start-up operation covering people, processes and systems.

Operational risk and other key risks are quantified using the following operational risk tools:

- Incident / Near Miss event Log
- Departmental Risk & Control Self-Assessments
- Scenario analysis
- Key Risk indicators

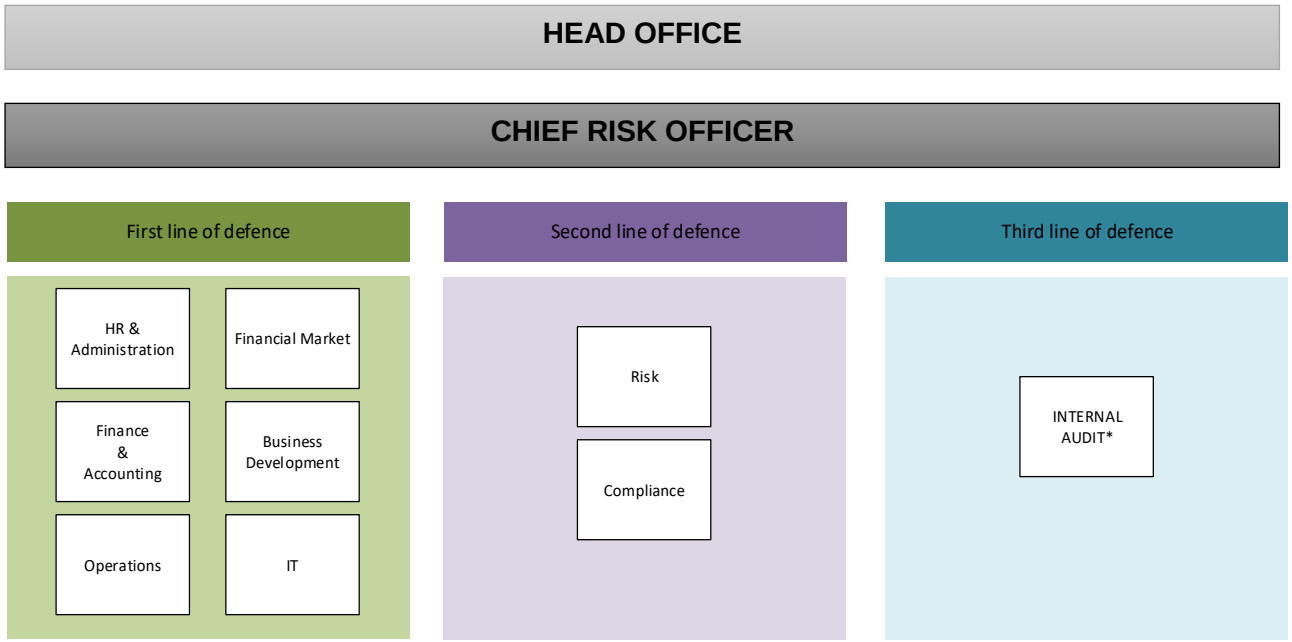
The above tools will be used to maintain the CNCBLB Risk Matrix which uses the Risk Scoring Methodology which takes account of both quantitative and qualitative assessments of the risks. This is monitored in terms of the KRIs which are outlined in the Operational Risk Management Policy. The suite of KRIs and calibration of KRIs will be reviewed at least bi-annually or as necessary by the ARCo.

# 5 Three Lines of Defence

## 5.1 Overview

The Branch's RMF at the highest level is based on a three lines of defence model. Under this model, responsibilities and accountabilities for risk management and compliance reside with the appropriate departments that undertake the day-to-day business activities, with appropriate policies, limits, checks and controls implemented by independent functions. A visual representation of this is shown in the figure below:

**Figure 1 Branch's Three Lines of Defence**




*Internal Audit will be provided by an external third-party on a fully outsourced basis.

## 5.2 Role of Head Office

HO sets the Branch's overall risk appetite, approves its risk management strategy and is ultimately responsible for the effectiveness of the risk management process and system of internal controls across the Branch.

HO strategy, policies and risk appetite are implemented in the Branch through the RMF. Where new HO requirements are issued, CNCBLB will amend the framework to maintain consistency, but the

condition that CNCBLB meets UK regulatory and legal requirements always takes precedence and HO policies will be amended as necessary to ensure compliance as stated in the DOA section.

HO is also directly involved in the three lines of defence through its annual audit of the Branch alongside any ad hoc audits, which are conducted by HO's Internal Audit, who will also receive any audit reports produced by external third parties related to the Branch.

### 5.3 Role of the Chief Risk Officer ("CRO")

The CRO (SMF 4) has an overarching responsibility to ensure that the Branch's RMF is fit for purpose and meets the requirements of the ManCo, HO and the Branch's regulators and external auditors. The CRO provides central oversight of risk management across CNCBLB and, supported by the second line functions, ensures that the full range of risks facing the Branch are properly identified, measured, monitored and controlled to minimise adverse outcomes.

The CRO is responsible for ensuring that the functions making up the three lines of defence are fulfilling the requirements of the framework, in particular the functions making up the first line, and engendering an awareness of risk and an appropriate risk culture throughout the Branch.

The CRO ensures senior management apply risk management perspectives to strategic decisions and provides independent advice in respect of all areas of risk. The CRO is also responsible for ensuring that the ManCo are kept fully advised with developments materially affecting the risk framework or risk profile of the Branch.

The CRO is a member of the following committees:

- ManCo;
- CCo (Chair);
- ARCo; and

  Asset and Liability Committee ("ALCo")

The CRO prepares a quarterly CRO Report for the HO Risk department covering the market, credit, operational and liquidity risk exposure of the Branch. A separate report is also prepared by the CCO and the MLRO which focuses on compliance and conduct risks. A summary of this report is included in the President's quarterly report to HO Senior Management.

### 5.4 First Line of Defence

The First Line of Defence ("1LOD") consists of all business and support units, and their individual staff, who are responsible for the day-to-day identification, mitigation, mitigation, management, and

monitoring of all risks arising within their functions. They are responsible, with support from the Second Line of Defence ("2LOD") functions, for developing and communicating appropriate procedures necessary to manage those risks within the policies laid out by the 2LOD and in accordance with the Branch's risk appetite.

The 1LOD has the following primary responsibilities:

- Identifying, analysing, reporting and prioritising ongoing and emerging risks arising in the business or function, in particular operational risk;
- Identifying and reviewing with the second line functions the risks arising in any new business or new products;
- Where applicable, mitigating or hedging these risks in accordance with CNCBLB's RMF;
- Ensuring the effectiveness of risk management and risk outcomes and allocating appropriate resources to execute risk management activities;
- Monitoring risk events and losses, identifying issues and implementing remedial actions to address these issues; and
- Reporting and escalating material risk events and losses and any other risk-related issues to the CRO.

The support functions, which include Operations, IT, and HR and Administration, may as part of their role, identify material risks or issues resulting from the activities of the departments. Where such risks or issues are identified, the support function is responsible for reporting them to the respective department's management and to the Risk Management department.

The Branch's first line functions include:

- Financial Markets;
- Business Development;
- Finance and Accounting;
- Operations;
- IT; and
- HR and Administration.

### 5.4.1 Financial Markets

All staff within the Financial Markets department will report to the Head of Financial Markets (SMF22) who in turn will report to the Vice President ("VP"). The Head of Financial Markets for the Branch will

also maintain a functional reporting line to HO's Financial Markets department. The Head of Financial Markets is a member of the following committees:

- ALCo; and
- ARCo (Permanent invitee for risk related matters).

The primary day-to-day responsibilities of the Financial Markets department include, but are not limited to:

- Executing trades on behalf of customers;
- Executing trades for internal hedging purposes;
- Checking and retaining trade documentation;
- Providing monthly management information ("MI") to the ALCo on financial markets activity;
- Market risk management;
- Asset and liability management;
- Keeping abreast of market trends and developments; and
- Communicating with customers (including relationship management).

Financial Markets - Treasury will also monitor liquidity measures as imposed by ALCo to ensure liquidity risk is managed:

Financial Markets – Treasury responsibilities will also include:

- Proposing to ALCo and, where appropriate, the Branch senior management, the policies, standards, methodologies, limits and procedures forming the framework for Market and liquidity risk management in the Branch, and ensuring that the framework is regularly reviewed and consistent with all HO requirements as well as meeting all applicable UK regulatory requirements;
- Establishing effective systems and procedures to measure and report independently the market and liquidity risks of the Branch;
- Managing the daily market and liquidity risk profile of CNCBLB;
- Test and be ready to implement a 'Liquidity Contingent Funding Plan'

### 5.4.2 Business Development

All staff within the Business Development department will report to the Head of Business Development (SMF 22) who in turn will report to the VP. The Head of Business Development for the Branch will also maintain a functional reporting line to HO's Corporate Banking department.

The Head of Business Development is a member of the following committees:

- ALCo; and
- ARCo (Permanent invitee for risk related matters).

The primary day-to-day responsibilities of the Business Development department include, but are not limited to:

- Drawing up draft terms of agreements (bilateral loans, syndicated loans, trade finance, and documents credit) for review by Risk Department and legal advisors where necessary;
- Negotiating the terms of transaction/deals/agreements;
- Evaluating credit proposals;
- Submission of credit proposals to the CCo;
- Monitoring credit limits within the first line of defence;
- Evaluating deposit account applications;
- Opening deposit accounts;
- Servicing deposit accounts;
- Retaining relevant documentation;
- Providing monthly MI to the ManCo and the ALCo on business development activity; and
- Sales and relationship building activities, such as:
    - Identifying sales leads;
    - Following up on leads provided by HO;
    - Attending networking events;
    - Pitching services to customers; and
    - Developing new initiatives.

### 5.4.3 Finance and Accounting

All staff within the Finance and Accounting department will report to the Head of Finance and Accounting (SMF 2) who in turn will report to the President. The Head of Finance and Accounting for the Branch will also maintain a functional reporting line to HO's Finance department.

The Head of Finance and Accounting is a member of the following committees:

- ManCo
- ALCo (Chair);
- ARCo and
- CCo.

The primary responsibilities of the Finance and Accounting department include, but are not limited to:

- Book keeping;
- Responsible for the day-to-day transactional accounting of the business;
- Outlining the policies and procedures that form the framework for accounting, regulatory and tax risk management in the Branch to the ARCo and, where appropriate ManCo;
- Providing daily MI on the liquidity risk profile of the Branch to Financial Markets, Risk department and senior management;
- Providing monthly MI on the liquidity risk profile of the Branch to ALCo, and HO including reports on any matters concerning material liquidity risk; and
- Providing reports on Branch's liquidity risk profile and other material liquidity risk matters to the HO.
- Providing daily MI on the liquidity risk profile of the Branch to senior management and the relevant departments;
- Providing monthly MI to the ALCo and the ManCo, and reporting any material risk matters to those committees or members of the senior management team in a timely manner;
- Reporting any material accounting, regulatory or tax risk matters to the ARCo and, where appropriate, the ManCo and HO;
- Reviewing the Branch liquidity, accounting, regulatory and tax risk frameworks with HO;
- Advising on the accounting and tax risk requirements of any new businesses or new products; and
- All recommendations made with respect to finance are consistent with HO requirements as well as meeting all applicable UK regulatory requirements.

Although a first line function for the Branch, the Finance and Accounting department also has second line responsibilities in regards to the delivery of accounting, regulatory and financial reports.

### 5.4.4 Operations

All staff within the Operations department will report to the Head of Operations (SMF 24) who in turn will report to the President. The Head of Operations for the Branch will also maintain a functional reporting line to HO's Operations department.

The Head of Operations is a member of the ARCo and is a permanent invitee for risk related matters.

The primary day-to-day responsibilities of the Operations department include, but are not limited to:

- Transaction reporting;
- Processing financial transactions (e.g. for clearing and settlement);
- Ensuring that credit facilities are disbursed only after contractual terms and conditions have been met and all required documents have been received;
- Liaising with Relationship Managers to ensure that the customer records are up to date;
- Entering into and managing all outsourcing (excluding IT) arrangements. This includes the overall risk management, governance and oversight of all outsourcing arrangement the Branch enters into including both with external as well as HO outsourcing arrangements; and
- Updating the Business Continuity Plan.

### 5.4.5 Information Technology (IT)

All staff within the IT department will report to the Head of IT (SMF 22) who in turn will report to the President. The Head of IT for the Branch will also maintain a functional reporting line to HO's IT department.

The Head of IT is a member of the ARCo and is a permanent invitee for risk related matters.

The primary day-to-day responsibilities of the IT department include, but are not limited to:

- Maintaining IT systems outside those hosted by HO;
- Maintaining infrastructure and devices used across the Branch;
- Investigating and resolving any IT related issues;
- Entering into and managing IT outsourcing arrangements (including that in place with HO for provision of IT infrastructure);
- Procurement of hardware and software and provision of these to employees as necessary;
- Risk assessment of IT related risks including cyber and operational risks arising (part of ongoing risk management process for ensuring completeness of the Risk Matrix of the Branch); and
- Responding to data retrieval requests.

### 5.4.6 HR and Administration

The HR and Administration function will report directly to the President to and the reason for this is to ensure alignment with a robust and effective RMF. The Head of HR and Administration department will maintain a functional reporting line to both the HR and the Administration Management department at HO.

The Head of HR and Administration will not be a member of any of the Branch committees.

The primary responsibilities of the HR and Administration department include, but are not limited to:

- Allocating appropriate resources to senior management risk activities;
- Ensuring all committee agendas and supporting documentation and provide to committee members in a timely manner;
- Ensure that all potential new Branch staff are correctly vetted and complete all components of the on-boarding process if successful in their application;
- Reporting any material staff risk matters to senior management; and
- Advising on the impacts of the regulators Training and Competence requirements.

### 5.5 Second Line of Defence

The second line comprises those functions with primary responsibilities for the independent risk and compliance oversight and monitoring. They propose to senior management the risk management and compliance framework within which the departments and the support functions manage the risks arising from their activities, monitor the implementation of the framework, including the general adequacy of the First Line's risk management activities, and report key risks to the ManCo and its sub-committees.

Heads of second line functions report on a periodic basis to HO on the activities of their respective areas in the previous quarter. This is to allow the Bank's Risk and Compliance functions to retain oversight of risk and compliance activities undertaken in respect of CNCBLB.

The Branch's second line functions will comprise the Risk Management Department and Compliance Department, with Treasury performing risk management activities in respect of liquidity risk management.

#### 5.5.1 Risk Management

All staff within the Risk department will report to the CRO (SMF 4), who in turn will report directly to the President. In addition to the CRO's local reporting obligations, a functional reporting line is also maintained to the Risk Management department at HO.

The CRO is a member of the following committees:

- ManCo;
- ALCo;

- CCo (Chair); and
- ARCo.

The primary responsibilities of the Risk Management department will include, but are not limited to:

- Proposing to the ManCo and, where appropriate, the ARCo, the policies, standards, methodologies, limits and procedures forming the framework for market, credit, liquidity and operational risk management in the Branch, and ensuring that the framework is regularly reviewed and consistent with all HO requirements as well as meeting all applicable UK regulatory requirements;
- Establishing effective systems and procedures to measure and report independently the market, credit, liquidity and operational risks of the Branch;
- Providing MI on the liquidity, market and credit risk profile of the Branch to the senior management team and the Financial Markets and Business Development departments;
- Providing monthly MI on the market, credit. liquidity and operational risk profile to ManCo;
- Providing monthly and quarterly stress-testing analysis for the Branch to ManCo;
- Reviewing the Branch RMF with the HO Risk department;
- Providing reports on the Branch's risk profile, asset portfolio and other material risk matters to the corresponding HO department;
- Providing independent credit risk analysis to Credit Committee and, where appropriate the corresponding HO department;
- Reviewing Branch market and credit risk limits at least annually; and
- Advising on the market, credit and operational risk requirements of any new businesses or new products.

### 5.5.2 Compliance

The Branch's Compliance Department will be responsible for implementing compliance related aspects of the RMF and in particular the Compliance Monitoring Program.

The CCO (SMF 16 & 17) acts in the capacity of the Branch Compliance Officer and Money Laundering Reporting Officer ("MLRO"). The CCO will report to the President and also maintain a functional reporting line to the HO Compliance department.

The CCO will be a member of the following committees:

- ARCo (Chair);
- CCo; and

- ManCo.

The primary responsibilities for the Compliance department will include but not be limited to:

- Proposing the policies and procedures forming the compliance framework within the Branch to the CCO;
- Ensuring the compliance framework is regularly reviewed and consistent with all applicable legal and regulatory requirements, which in turn will be reviewed annually by the ARCo to ensure continued effectiveness and appropriateness;
- Keeping up to date with applicable legal and regulatory requirements and obligations and ensuring these are communicated to the senior management team and impacted staff in a timely and effective manner;
- Advising on regulatory requirements of any new business or new products;
- Single Customer View ("SCV") file generation / oversight of the ongoing compliance with SCV requirements;
- Providing compliance, anti-money laundering and financial crime training to the Branch's management, business heads and other staff, and induction training to new joiners;
- Monitoring the Branch's regulated activities to identify situations in which the Branch has not acted in accordance with its regulatory responsibilities and escalating any issues to the ManCo, and if appropriate the regulators;
- Monitoring news of relevant enforcement actions by the UK or Chinese regulators and communicating these and any necessary actions to the senior management team;
- Responsible for the interaction with the PRA and FCA; and
- Promoting a good compliance culture by engaging staff from all around the business.

### 5.5.3 Legal

Due to the size of the Branch there will be no legal function.

Instead external legal advisors will be engaged on an ad-hoc basis as required. The Head of Business Development or the CCO, following approval from the President (unless the due diligence requirements under the Outsourcing Policy are triggered), will be required to manage the relationship with such third-party providers.

## 5.6 Third Line of Defence

The Third Line of Defence ("3LOD") consists of those functions with responsibility for providing assurance on the adequacy, appropriateness and effectiveness of the Branch's first and second line

of defences. In the case of CNCBLB, no External Auditor is required given its status as a Branch of a Non-EEA branch.

This means the Internal Audit ("IA") Function will be the sole 3LOD within CNCBLB and this will as previously noted be outsourced to a third-party IA Service Provider. The third line functions and their responsibilities are detailed below.

### 5.6.1 Local Internal Audit Function

IA will be outsourced to an external third-party provider in accordance with the Branch's outsourcing framework.

The President will be responsible for the relationship with the IA provider whereas the ARCo will be responsible for the oversight and challenge of the deliverables produced by the IA provider. The appointment of the third-party will be subject to the provisions of the Outsourcing policy and will require clear Service Level Agreements and Key Performance Indicators ("KPIs") to be put in place.

The primary responsibilities of the outsourced Internal Audit function will be as follows:

- Reviewing and maintaining a record of the Audit universe to ensure all Branch risks are identified, assessed, and prioritised, and planned audits are performed with the appropriate frequency;
- Developing and proposing to the ARCo, the annual Branch Audit Plan, and agreeing the plan with the HO Audit Department. Internal Audit considers any management directives, resolutions or material changes to the business or to the risk management & compliance framework that could be relevant to its activities and updates its audit plan accordingly;
- Carrying out audit reviews in accordance with the annual audit plan, primarily focusing on assessing the design, adequacy and operating effectiveness of key internal controls, including adherence to policies and procedures;
- Presenting final audit reports to the ARCo for review and agreement on management actions. Reports include a description of the audit work performed and findings; highlighting any major deficiencies, laying out the remedial management actions and setting target completion dates.
- Reviewing regularly with ARCo the progress made on agreed management actions on all audit reports;
- Reporting any material audit matters to ARCo and, where appropriate, senior management and HO; and
- Reviewing the Branch's internal audit arrangements with HO.

### 5.6.2 HO Internal Audit Function

HO's IA team will carry out periodic reviews of the Branch as part of HO's own IA programme and to allow HO to confirm compliance with requirements stipulated from China such as those set out in the DOA. For completeness, the range of responsibilities of the HO IA function are set out below:

- Organising the Bank's annual internal audit;
- Drafting internal audit policies and procedures as well as the Bank's quality control standard;
- Auditing the accuracy and reliability of the Bank's accounting records and financial reports;
- Auditing the Bank's IT system design, operation and development as well as management and maintenance;
- Auditing the Bank's risk related capital assessment systems;
- Auditing the Bank's operational and management performance at all level;
- Auditing the soundness and effectiveness of the Bank's domestic subsidiaries and overseas entities' internal control as well as risk management;
- Coordinating the Bank's resource in terms of inspection and supervision, integrating the Bank's inspection and supervision plan;
- Training the Bank's internal auditors to ensure their professional competence;
- Monitoring the rectification and implementation of internal and external issues;
- Maintaining the communication with regulators and external auditors;
- Coordinating external inspection;
- Tracking and evaluating of regulatory feedback; and
- Reporting to the Board of Directors, Board of Supervisors and Internal Control Committee.

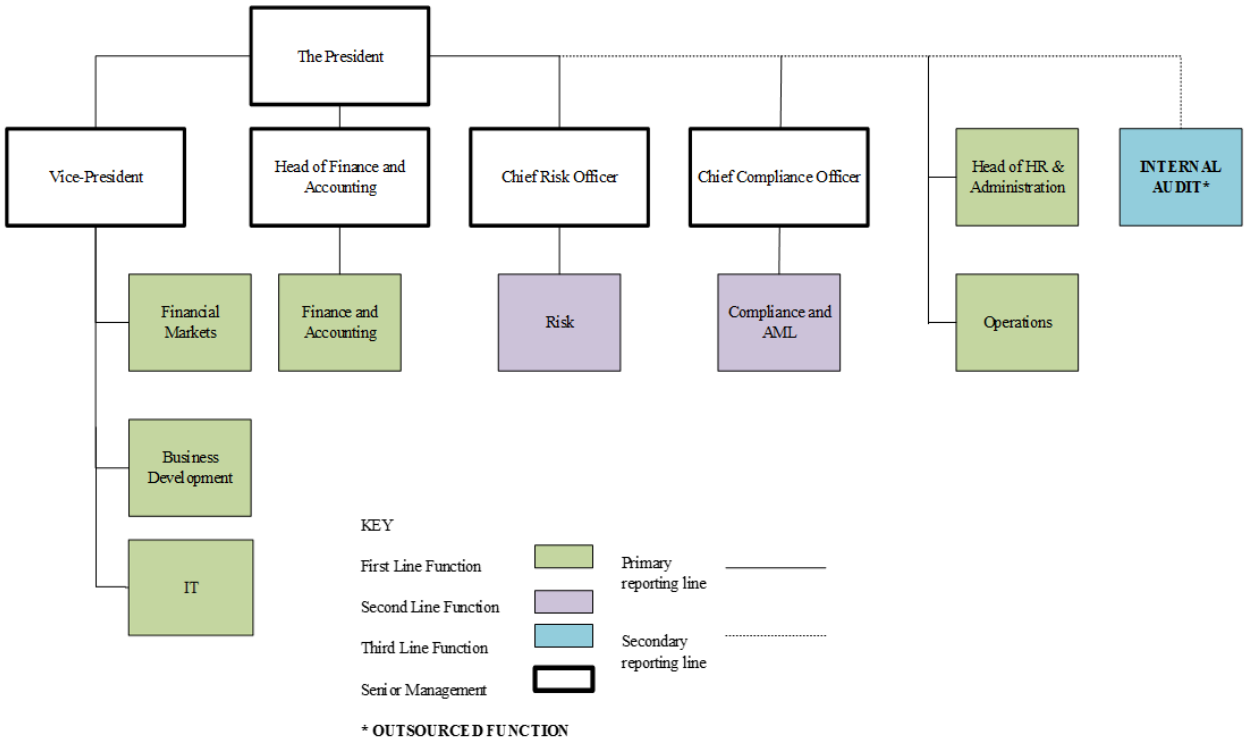
### 5.6.3 External Audit

The London Branch is not required to have an external auditor, as it is covered through the HO audit. The Branch will support HO in group activities related to external audit as required.

## 6 CNCBLB organisational structure

The organisational structure within the Branch has been designed to align itself to the TLOD. As a result, other than the reporting lines into the President from across the senior team, all other teams are placed within a single line of defence. This ensures alignment of functional objectives and that potential conflicts of interest are avoided.

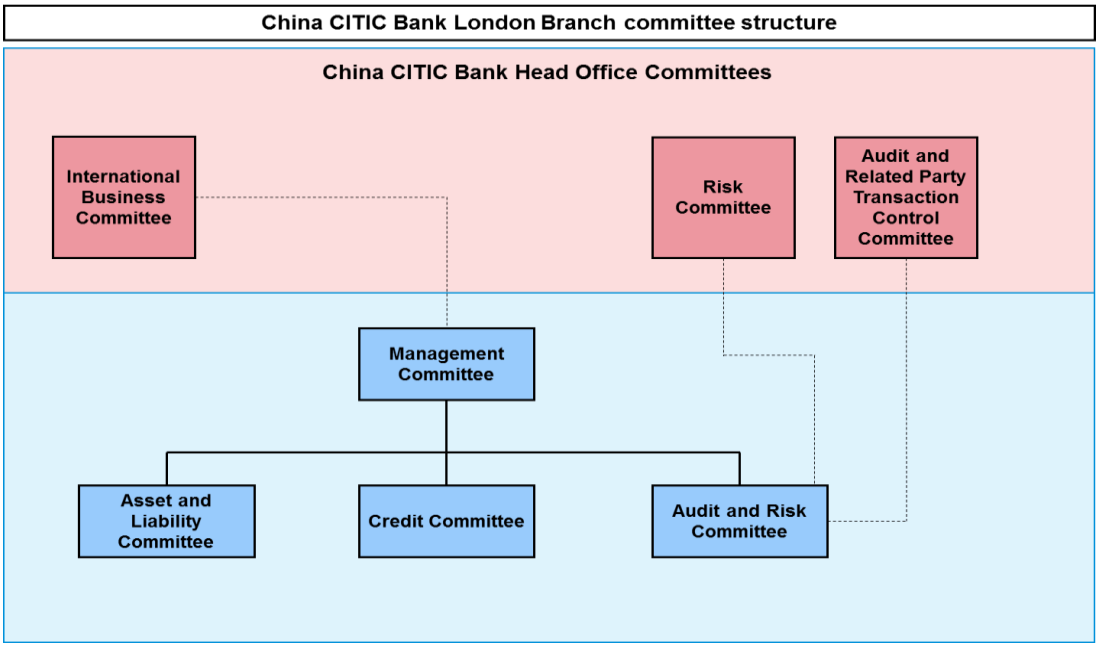
## 6.1 Branch Organisational Structure




## 6.2 Committee Structure Overview

The full committee structure of the Branch, as well as their interaction with HO committees is illustrated below. Each committee that reports into the ManCo assists in taking responsibility for specific aspects of the RMF.

### Branch Committee Structure



### 6.3 Management Committee

The ManCo is the most senior committee within the Branch. It is constituted to support the President deliver against the strategy of the branch in accordance with the DOA. ManCo derives its mandate from the President's DOA.

The responsibilities of the ManCo (see ***Appendix C*** for full Terms of Reference) include and assess the performance of all activities undertaken by the Branch to ensure these are in line with the HO approved strategy and risk appetite as well as regulatory requirements and expectations:

- Set the local strategy based on the Delegation of Authority from Head Office ("HO") to the President;
- Set local risk limits and thresholds based on recommendations from sub-committee;
- Consider all correspondence with the UK regulators (the Prudential Regulation Authority and the Financial Conduct Authority);

  Approve the risk management framework overall as well as its component parts (e.g. the compliance monitoring programme and the anti-money laundering ("AML") processes) are appropriate and fit for purpose given the size, nature and complexity of activities undertaken. This will include the periodic review of the Risk Matrix as well as the Risk Appetite Statement ("RAS");
- Approve all other policies implemented across the Branch based on recommendations from sub-committees where responsibility for approval rests with the ManCo;
- Act as escalation point for all sub-committees;
- Approval of all risk limits and thresholds in accordance with the Branch RAS;
- Review the overall risk profile of the Branch on a monthly basis;
- Review MI that is produced by all functions and committees
- Anticipate macroeconomic changes which could affect operations and formulate strategies to effectively mitigate the risks arising from such changes; and
- Review and approve the annual Internal Audit plan.

The ManCo will comprise:

- The President (Chair);
- VP;
- CRO;
- CCO; and
- The Head of Finance and Accounting.

### 6.4 Asset and Liability Committee

The ALCO receives its mandate from the ManCo. Within the terms of the President's DOA, ALCO's primary responsibility will be to review and monitor market risk, the Branch's funding, liquidity management and balance sheet structure.

The responsibilities of ALCO (see ***Appendix D*** for full Terms of Reference) include:

- Establish, propose and oversee the assets and liabilities management strategies of the Branch;
- Guide, oversee and review the Branch's Market Risk and Liquidity Risk Management Policy;
- Review earning exposure as well as asset and liability risks arising from the business undertaken by the Branch and the shape of the balance sheet;
- Recommend to the Audit and Risk Committee ("ARCo") relevant limits, management review trigger limits, control ratios and guidelines in accordance with the Branch RAS as applicable to market and liquidity risk and asset and liability management more generally;
- Recommend the strategies, organisation, method of analysis and system support for the management of the assets and liabilities of the Branch;
- Review periodically the market and liquidity risk profile of the balance sheet;
- Assess periodically the Branch's overall ability to meet liabilities as they fall due;
- Define and recommended to ManCo the Branch's funding strategies in respect of deposit taking and debt issuance;
- Review and recommend any changes to MI and metrics used for the measurement of asset and liability performance; and
- Oversee and challenge performance of budget against actual financial returns.

The ALCO will comprise:

- Head of Finance and Accounting (Chair);
- President;
- VP;
- CRO;
- Head of Financial Markets; and
- Head of Business Development.

Although not a regularity, should any other departments wish to attend the ALCO, approval will have to first be provided by the Chair. Any additional attendees to those mentioned above will not be given the right to vote on decisions made at the ALCO.

Under the authority delegated to ALCO, decisions made at the committee do not need to be ratified by the ManCo. However, any material issues raised at committee meetings must be escalated to the ManCo.

### 6.5 Audit and Risk Committee

The ARCo will receive its delegated authority from the Branch's ManCo. Its role is to ensure effective oversight of the Branch's RMF and to assess and review the outputs of the outsourced Internal Audit department.

The responsibilities of the Committee (see ***Appendix E*** for full Terms of Reference) will include

- Assess the Branch's risk profile on a periodic basis including the Compliance Risk profile:
- Challenge the completeness of the Risk Matrix and the relative risk scores attributed to individual risks;
- Assess the adequacy of the Risk Management Framework relative to the activities undertaken by the branch and the requirements and expectations of the Regulators;
- Review the risk management framework and conform that the related policies and procedures are properly implemented, maintained and fir for purpose and report any findings to the ManCo as required;
- Review proposed changes to the RMF and the supporting policies before submitting to the ManCo for final approval;
- Assess the impacts of any breaches to RAS or risk management related policies;
- Review the Compliance Monitoring Programme to ensure its completeness and the effectiveness of it implementation;
- Review scope of annual Internal Audit Plan;
- Review and challenge the adequacy of the Internal Audit Methodology to be deployed by the third-party outsource provider on behalf of CNCBLB;
- Review and monitor the remedial action taken following completion of individual internal audits; and
- Review new products proposed in line with the New Products Approval Policy.
- Report to the HO Risk Committee and Audit & Related Party Transaction Control Committee to support HO oversight activities.

In order to ensure the three lines of defence model to be implemented by the Branch is effective, the ARCo will split the committee to discuss *audit* and *risk* matters separately. Therefore, each member has been allocated one of the following roles; Risk, Audit or Risk and Audit. Consequently, those only required for the Risk section of the ARCo will be required to leave once Audit specific matters are being discussed and vice-versa.

The members of the ARCo will be:

- CCO (Chair - Risk and Audit):
- President (Risk and Audit);
- VP – (Risk and Audit):
- CRO – (Risk and Audit):
- Head of Finance and Accounting (Risk and Audit);

Permanent Invitees:

- Head of Operations (Risk);
- Head of IT (Risk);
- Head of Business Development (Risk); and
- Head of Financial Markets (Risk).

The individual who is ultimately responsible for the provision of Internal Audit outsourced services to CNCBLB (e.g. a Partner of an accounting firm) will attend the Audit part of the ARCo meetings annually or as required by the committee. This will be on an invitation only basis and subsequently will not be attributed voting rights.

Decisions made by the ARCo must be ratified by the ManCo and any material issues raised at meetings must be escalated to the ManCo.

### 6.6 Credit Committee

The Credit Committee (“CCo”) has been granted delegated authority by the President to oversees credit risk within the terms of the HO DOA; to review and approve credit applications and set credit limits for individual counterparties and groups.

The primary responsibilities of the CCo (see ***Appendix F*** for full Terms of Reference) include:

- Assess periodically the effectiveness of credit risk management arrangements in place to monitor credit risk arising in the Branch across the Financial Markets and the Business Development departments.
- Assess and approve all credit application for loans/facilities in line with the DOA, RAS and Credit Approval and Credit Risk Management policy;
- Arrange for submission to HO Credit Committee any credit application which are within the RAS but outside the DOA for further consideration and/or approval;
- Make recommendations to the ManCo on the credit risk policy and Branch strategy, where appropriate;
- Act as escalation point for risk and the business for all credit events (such as deterioration of risk profiles, losses or write-offs);
- Assess periodically credit documentation standards;
- Review and approve credit limits on an individual, group, sector and country basis;
- Review and escalate, where appropriate, breaches of credit limits and escalate to ManCo accordingly; and
- Recommend Loan Loss Provisions to the ManCo.

The CCo will comprise:

- CRO (Chair);
- President;
- VP;
- Head of Finance and Accounting; and
- CCO.

All members of the committee have the right to vote unless a conflict relative to an individual matter exists. Any conflicts must be declared at the beginning of each committee meeting.

## 7 Risk Identification and Assessment

This section summarises the business activities of CNCBLB, and the processes used to identify and assess the risks to which the Branch will be exposed as a result of those activities. The overarching objective of the Branch RMF is to ensure that key risks are properly identified, assessed, mitigated or controlled and reported. This section sets out the key risks faced by the Branch and is based upon the assessment in the Risk Matrix, and summarises how they are managed.

The key risks for the Branch include, but are not limited to:

- Strategic / business;
- Credit;
- Market;
- Operational;
- Liquidity;
- Compliance & Regulatory; and
- Legal.

### 7.1 Strategic/Business Risk

Strategic/Business risk is the risk of an external or internal event preventing the Branch from achieving its objectives. The Bank's reputation is fundamental to the Bank being able to carry on business.

The Branch therefore expects all employees to be aware of how their actions or omissions could impact the Bank's reputation and to ensure that they do not adversely impact the Bank's reputation.

It is the responsibility of the individual managers of each of the various business areas to be aware of the impact that an action or omission could have on the Branch's reputation and to ensure that the Bank's reputation is adequately and properly protected. The Branch has identified the following sources of strategic risk to its business:

- **Economic risks:** changes in interest rates, global growth/decline and other macroeconomic risk factors;
- **Competition:** Competition from other Chinese banks based in the UK or Europe, and from other Chinese financial institutions looking to develop their presence in Europe;

- **Significant Losses:** Significant losses, particularly from credit events, but also from market movements, or regulatory action could severely impact the Branch's ability to achieve its objectives;
- **Political and Regulatory Risk:** For instance consequences of Brexit or a change in the regulatory approach to non-EEA branches in the UK; and
- **Staffing:** The Branch has a limited number of staff to carry out its business.

The Branch has the following mitigants in place:

- Discussion of emerging issues in all committees;
- Staff meeting discussions;
- Periodic video conferencing with HO;
- Network meetings with related parties;
- Policy guidelines;
- Regulatory inputs;
- Interactions with external skilled persons/consultants;
- Internal/external audit reports.

### 7.2 Credit Risk

Credit risk is the risk of loss due to one or more counterparties/borrowers/issuers defaulting on, or otherwise being unable to fulfil, their contractual obligations. Credit exposure will be generated by the following products:

| Business Activity | Products | Country Risk | Obligor Risk | CP Risk | Issuer Risk | Pre-Settlement | Settlement Risk |
|---|---|---|---|---|---|---|---|
| Financial Markets | • Money Market instruments | √ | | √ | | | √ |
| | • Repurchase Agreements | √ | | √ | | | √ |
| | • FX spot | √ | | √ | | √ | √ |
| | • FX Forwards / Swaps | √ | | √ | | √ | √ |
| | • Interest Rate Swaps | √ | | √ | | √ | √ |
| | • Liquid Bonds | √ | | | √ | | |
| | • Corporate Bonds | √ | | | √ | | |

| Business Activity | Products | Country Risk | Obligor Risk | CP Risk | Issuer Risk | Pre-Settlement | Settlement Risk |
|---|---|---|---|---|---|---|---|
| Banking | • Payment Services<br>• Bilateral loans<br>• Syndicated Loans<br>• Project Finance<br>• Asset backed structured finance<br>• Bill and Telegraph Transfer financing<br>• Letters of Credit<br>• Letters of Guarantees<br>• Forfeiting/Receivable financing | √<br>√<br>√<br>√<br>√<br>√<br>√<br>√<br>√ | √<br>√<br>√<br>√<br>√<br>√<br>√<br>√<br>√ | | | | √ |

**Definitions**

CNCB LB defines credit risk management in 5 categories

1. **Country Risk** - risk that a foreign government will default on its financial commitments and/or the degree to which political and economic unrest affects doing business in a particular country.
2. **Obligor Ris**k - also known as a debtor, is a person or entity who is legally or contractually obliged to make all principal repayments and interest payments on outstanding debt
3. **Counterparty Risk** - the risk to each party of a contract that the counterparty will not meet its contractual obligations. In most financial contracts, counterparty risk is also known as default risk.
4. **Issuer Risk** – the legal entity that issues a financial instrument, any investor in the financial instrument incurs not only the market *risk* associated with any type of investment, but also an *issuer*-related default *risk*.
5. **Pre-settlement risk** – the risk that a counterparty defaults prior to maturity of a transaction which results in a market-to-market (plus credit add-on) exposure (replacement cost)
6. **Settlement Risk** – unless settled 'Delivery verse Payment' ("DVP") through an approved clearing hose/exchange, settlement risk is the risk that a counterparty or intermediary agent fails to deliver cash or a security as per the agreement.

The following credit risk mitigants could be employed by the Branch to help manage its exposure to credit risk:

- Avoiding concentrations of risk by limiting exposures to individual counterparties/borrowers and groups, and diversifying exposure across different counterparties, thereby reducing the impact of a single counterparty default;
- Ensuring robust initial and ongoing credit analysis of counterparties, groups and countries;
- Setting transactions through assured payment systems or on a delivery-versus-payment basis;
- Limiting exposures to individual countries and industry sectors, and diversifying exposure across different countries and sectors to the extent that it is possible within the constraints of the overall business model of the Branch;
- Setting limits on tenures of transactions with counterparties;
- Utilising netting and collateral agreements where possible;
- Ensuring robust documentation of transactions, including setting appropriate covenants, where possible; and
- Where possible, obtaining HO or third-party guarantees to reduce the risk of loss.

For detailed information on how the Branch's credit risk is managed' reference should be made to the Branch's ***Credit Approval and Credit Risk Management Policy***.

### 7.3 Market Risk

Market risk refers to the risk of on-and off-balance sheet businesses of a bank incurring losses due to unfavourable changes in market prices (including interest rate, exchange rate, stock price and commodity price). Market risk impacts both the Branch's trading and non-trading parts of the business, which results in interest rate, currency risk, share price and commodity price risk (although not relevant to the planned activities of the branch).

The Branch has identified two key types of market risk; interest rate risk and exchange rate risk, both of which are defined below:

#### 7.3.1 Interest Rate Risk

Interest rate risk refers to the risk of losses to overall earnings and economic value of bank accounts resulting from unfavourable changes in factors such as interest rate and maturity structure, including re-pricing risk, yield curve risk, benchmark risk and option risk. The Branch will manage its interest rate risk in accordance with the risk appetite in order to ensure steady growth of both net interest income and economic value within the acceptable range of interest rate risk.

### 7.3.2 Foreign Exchange Risk

Foreign Exchange ("FX") Risk refers to the risk of on and off-balance sheet businesses of a bank incurring losses due to unfavourable changes of exchange rate. The Branch will measure exchange rate risk mainly through the analysis of foreign exchange exposures that consist of trading and non-trading exposures, including trading exposure that mainly results from the position in foreign exchange trading and non-trading exposure that mainly arises from foreign currency capital and foreign currency profit.

The risk management methodology of interest rate and the exchange rate risk that the Branch will implement is the 'Value at Risk' methodology ("VAR") used by HO. VAR covers risk identification, measurement, monitoring and reporting of position risk, thereby controlling market risk within an acceptable range and maximising risk-adjusted returns. The VAR system will also provide back-testing and stress testing of CNCBLB's market risk positions.

The Branch will also manage its market risk by:

- Matching foreign current denominated assets with corresponding foreign currency denominated liabilities;
- Making appropriate use of financial derivatives to hedge positions;
- Setting Intraday and overnight FX open position risk limits;
- Setting interest rate maturity and gap mismatch limits; and
- Ongoing independent assessment of market conditions.

For detailed information on how the Branch's market risk is managed' reference should be made to the Branch's ***Market Risk Management Policy***.

### 7.4 Operational Risk

Operational risk is the risk of an economic loss, a disruption to business, an adverse impact on reputation or on customer relationships or of legal action arising from inadequate or failed internal processes, people and systems. Operational risk will generally occur due to either inadequate or failed internal processes, staff, IT systems or other external factors. Within this broad classification, the Branch will identify a number of categories of operational risk:

| OPERATIONAL RISK | BASEL EVENT TYPE | DESCRIPTION |
|---|---|---|
| PEOPLE RISK | Internal Fraud | Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/ discrimination events, which involves at least one internal party |
| | External fraud | Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party |
| | Employment Practices and Workplace Safety | Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/ discrimination events |
| PROCESSESS RISK | Clients, Products & Business Practices | Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product |
| | Execution, Delivery & Process Management | Losses from failed transaction processing or process management, from relations with trade counterparties and vendors |
| SYSTEMS RISK | Business disruption and system failures | Losses arising from disruption of business or system failures |
| EXTERNAL RISK | Damage to Physical Assets | Losses arising from loss or damage to physical assets from natural disaster or other events |

The Branch is committed to identifying, assessing, monitoring, controlling, mitigating, and reporting operational risk through an operational risk management framework. Besides, the Bank will implement effective control measures to reduce the loss of operational risk, promote the construction of operational risk management system and constantly improve the operational risk management mechanism of dynamic management and continuous improvement.

The four operational risk tools used to identify, measure, manage and report operational risk are:

1. Incident/Near miss log (includes root cause analysis, corrective and preventative actions)
2. Risk & Control Self-Assessments (Departmental risk identifications and controls in place)
3. Key Risk Indicators (monitoring and reporting of key risks to senior management)
4. Scenario analysis (conduct and non-conduct risk scenarios that could negatively impact CNCBLB)

For detailed information on how the Branch's operational risk is managed' reference should be made to the Branch's ***Operational Risk Management Policy***.

Operational risk will also cover the following risk categories:

**IT Risk**

The Branch defines IT risk as the failure of computer and infrastructure related to IT. It is the risk of a threat exploiting vulnerability of an IT based asset or group of assets which will in turn cause harm to the Branch and/or wider HO and its clients. The risks associated with information security and information technology are managed by the following control processes:

**Information Security Management**

Head Office has a dedicated Information Security Group that drives the Bank's information security programme. This Group develops and implements policies and standards covering all aspects of information security in line with ISO17799, the internationally recognised Code of Practice for Information Security Management.

**Cyber Security**

The Bank uses various anti-virus software to prevent malicious attacks. All data is replicated real-time to the Head Office back-up systems which is tested at least annually to ensure replication supports the business requirements. Scenarios relating to cyber-attacks will be included in the business continuity tests.

**Systems Access**

Access to all of the Branch/Bank's systems require authorisation from appropriate levels of line management and periodic checks are undertaken to ensure that access rights remain in line with requirements.

**Systems Development**

All new systems or changes to existing systems require approval by Head Office.

***Outsourcing Risk***

The Branch considers outsourcing risk as the failure to have effective oversight of existing and proposed outsourcing arrangements in place. CNCBLB is aware that it undertaking outsourcing activities, the process gives rise to several risks that need to be appropriately mitigated:

- **Business Strategy Risk:** The risk arising from erroneous business decisions, failure to implement decisions or lack of responsiveness to industry changes. This risk is a function of the compatibility of organisation's strategic goals, the business strategies developed to achieve those goals, the resources deployed against these goals and the quality of implementation. The Service Provider may conduct business on its own behalf, which is inconsistent with overall strategic goals of the Branch;
- **Reputational Risk:** The risk arising from negative public opinion. The risk may expose the institution to litigation, financial loss or a decline in customer base. Poor service from the Service Provider and its customer interaction not being consistent with the overall standards of the Branch;
- **Legal and Compliance Risk:** The failure of a Service Provider in observing with UK legal and regulatory requirements can lead to levying of fines, penalties or punitive damages, resulting from supervisory actions. Additionally, risks arise arising from whether or not the Branch has the ability to enforce the contract;
- **Operational Risk:** This risk arises due to technology failure, fraud, error, inadequate financial capacity to fulfil obligation and/or provide remedies;
- **Exit Strategy Risk:** This could arise from over–reliance on one firm, the loss of relevant skills in the Branch itself preventing it from bringing the activity back in-house and contracts entered into wherein speedy exits would be prohibitively expensive; and
- **Concentration and Systemic Risk:** Due to lack of control of the Branch over a Service Provider, more so often when overall banking industry has considerable exposure to one Service Provider. Failure of a Service Provider in providing a specified service, a breach in security/confidentiality, or non-compliance with legal and regulatory requirements, among others may lead to reputation / financial losses for the Branch and may also result in systemic risks within the banking system in the country.

**Business Continuity Planning**

***Contingency and Disaster Recovery***

China CITIC Bank HO has built a "Two Cities Three Centres" disaster recovery ("DR") system. All three centres have the necessary network, server and storage deployed. The three centres have different objectives:

- The main production centre is located at Chaoyangmen, Beijing, where all production systems are installed;
- The "same-city" centre is located at Jiuxianqiao, Beijing, where some management systems and all same-city DR systems are deployed; and
- The remote centre is located in the city of Xi'an, to support the remote switchover of key systems in extreme conditions.

In the HO's "Two cities three centres" DR system, the same-city DR is implemented at an application level, and will gradually evolve to ultimate provide "dual active" infrastructure. All significant systems can be switched over to same-city DR promptly, to meet the requirements of major accidental scenarios. The remote DR is used to help the Bank operate in extreme disasters. The core banking system and key channel systems can be switched over to the remote centre. All other important systems duplicate data to the remote centre as well.

In the DR environment of HO, IT systems are classified based on the "cost-risk balance" principle. Different DR strategies and solutions are constituted according to the business characteristics of different business systems.

- **Core banking system**: The core banking systems (including overseas core banking system) are running on IBM System platform, and protected by MIMIX solution. Application data is copied from one production machine to 3 different standby machines (located in 3 centres). The core system can be switched to the same-city centre within one minute.
- **Client-facing business systems**: Important business systems for external clients will deploy applications in both centres in Beijing running in a "dual active" mode. There will be no need to switch the applications if one site fails. The underlying databases are protected by disk replication or DB replication, which requires 10-20 minutes to switch over to DR. The overseas counter system, international trade finance system and financial market system will all be protected by this kind of solution.
- **Network**: The two data centres in Beijing are connected by raw fibre cable and DWDM to implement synchronous data replication and fast system switchover. The remote centre is connected by dedicated communication lines. A same-city network "dual active" solution is

promoted to CNCB branches, to achieve the ability of instant network failover between a Branch's two server rooms. The London Branch will also adopt this network DR solution locally.

The CNCB HO has established a comprehensive emergency management system, including contingency plans, DR drills, and emergency handlings.

- **Contingency plans**: Standard contingency plan templates are designed to cover all aspects, e.g. applications, network, storage, and IT infrastructure. And the contingency plans will be updated promptly after each system change, to keep their validity;
- **DR drills**: The HO will plan for DR drills in the beginning of each year. The drills include production system switchover, desktop drills and covers different scenarios like same-city failover, remote failover, accident recurrence and failure simulation. Each drill will involve business departments. The detailed process will be recorded, and all issues found will be retrospectively corrected; and
- **Emergency handlings**: Complete procedures are defined to deal with emergency situations. The emergency triggering conditions, and corresponding procedures including notification, organisation, reporting, decision, are all specified.

The IT systems used by CNCBLB are general production systems that will be shared by all CNCB overseas branches. Hence those systems are all installed in the Beijing production centre, with their backup systems in the same-city centre and remote centre. All system changes will be submitted by CNCBLB (or other overseas branches) staffs to the HO Data Centre where the actual change operation will be executed. In the event of DR drills, or system faults, the CNCBLB will cooperate with the Data Centre for the system emergency handling process.

Although no production systems are physically installed in London, CNCBLB will deploy network infrastructure and some local supportive IT systems (e.g. virtual desktops and event monitors) to support the local daily business operations. To ensure continuous business service, CNCBLB will also plan for disaster recovery arrangements, including establishing a backup server room in London. In the backup server room, standby networking, server and storage devices would be installed. Important data of the Branch (primarily shared documents within the branch) is copied from the production server room to the backup server room. If the London production server room fails, the IT network and services will be restored in the backup server room and normal business services will resume.

Non-IT BCP

Naturally, BCP is not merely an IT related exercise as DR scenarios could arise where the IT infrastructure is fully functional but Branch staff if unable to make use of the Gresham Street offices. For these purposes a range of non-IT BCP arrangements have been implemented as set out below.

DR Site

The CNCBLB DR site will be situated four miles away at:

01MC3A, 3rd floor, LD8, Harbour Exchange Square, Isle of Dogs, London, E14 9GE.
The alternate office location has been chosen to be sufficiently far away from the main office such the likelihood of both sites being affected simultaneously is extremely remote.

Branch staff will have full access to the Bank's network and to all the business systems.

Non-IT Fail-over process

The London Branch Non-IT BCP process is as follows:

- In case of a severe office damage, Branch management and business departments can work at the DR site to run daily business as required (after successful IT failover):
    - HO IT systems can be accessed;
    - Trading platforms can be connected;
    - Email and HO office systems can be accessed;
    - Branch shared documents available;
    - Internet available; and
    - Working space available
- After a successful DR fail-over, all Branch business can be done at DR site, although it may be conducted with a degraded performance. The Branch's business people can work there until primary site (office) resumes, when a failback will first be performed by IT department to update new local data back to office. London Branch will conduct local DR/BCP tests to verify the DR/BCP procedures, at a frequency of no less than once per annum;
- Ensure payments continuity (all payments, bar some minor expenses, are made via SWIFT deployed at HO) with CITIC HO's assistance as appropriate. In case we later encounter unforeseen difficulties in establishing connection to the SWIFT system in good time for execution of the current day's money market payments, advise our contacts at our correspondent banks and agree alternative methods of accepting payment instructions;

- Check cash positions. In the event that the Banking system is unavailable for some time, the cash positions must be determined by contacting our correspondent banks as appropriate;
- Organise staff attendance bearing in mind the space available, immediate needs and later requirements; and

When CNCBLB's banking and computer systems are restored, print balance sheet and main USD statement to check that data and system is up to date.

***Conduct Risk***

Conduct risk is the risk of customers being treated unfairly or being disadvantaged by the actions of the Branch and includes the potential for conflicts of interest between the Branch, HO and its customers. It also includes the risk of failing to meet market rules or standards, or general laws covering the Branch's activities.

The Branch will operate in the wholesale markets only. The Branch has therefore developed a conduct risk policy framework to ensure conduct risk can be appropriately identified, monitored and managed across the identified risk universe.

The Branch identifies several key sources of conduct risk in its business:

- **Failure to meet, or take into account, customer needs**: selling inappropriate products to customers or inadequate ongoing review of products and services for customers, giving inappropriate advice to customers, and/or providing misleading or non-compliant marketing material;
- **Failure to treat customers fairly or to act in their best interests**: providing misleading marketing information on products, pricing products inappropriately, failing to provide best execution of customer orders, failing to deal appropriately with customer complaints;
- **Failure to meet required market standards**: intentionally or unintentionally failing to meet market rules or standards, or the general regulatory or legal framework within which business is carried out, including anti-bribery and corruption legislation or sanctions rules; failure to prevent market manipulation or insider trading by Branch staff;
- **Failure to implement adequate systems infrastructure**: in particular, adequate to meet customers' needs and execute and administer products/services effectively; and
- **Failure to deal with conflicts of interest**: failing to deal with conflicts of interest with/between customers and/or with HO.

The Branch has a zero tolerance for conduct risk and the senior management recognise that the governance and the underlying culture of the organisation is central to ensuring conduct risk is managed and mitigated appropriately.

Conduct risk can occur at a number of points on the customer journey, from the design of products, to the way products are sold, to the ongoing servicing of customers' needs. It can arise in all of the Branch's business and corporate activities. The Branch will mitigate its conduct risk by establishing a clear framework of policies and procedures for dealing with customers and for transacting in markets, and providing appropriate training for all staff in these policies and procedures and in the standards expected of them when dealing with customers and markets. The first line of defence for conduct risk is formed of the departments and supporting functions in which the conduct risks arise.

In order to manage conduct risks effectively, each department and supporting function are required to:

- Ensure that conduct risk is taken into account in all business decisions and that appropriate judgement is exercised on the impact of Branch's actions on the customer or market integrity;
- Ensure that staff incentives promote appropriate behaviour;
- Identify and quantify the sources of conduct risks in their area;
- Identify actions to mitigate those conduct risks and enact policies and procedures to implement those actions;
- Communicate these risks and mitigating actions to the Compliance department and the CCO if necessary;
- Ensure that all staff undertake regular conduct risk training; and
- Identify any conduct risk event and communicate these to the Compliance department.

As a control function, the Compliance department is responsible for carrying out the following checks on a regular basis:

- Documents the conduct risks identified and communicated to it by the departments and supporting functions, and any mitigating actions;
- Challenges the departments and supporting functions to ensure all conduct risks are identified and that the potential conduct impact of significant business decisions has been fully considered;
- Maintaining the Conduct Risk Matrix and a record of, and reporting on, conduct risk events, and regularly reports these to ARCo and senior management; and

- Documents conduct risk events and regularly reports these to ARCo and, where appropriate, to the senior management team, ManCo, the President and HO.

The CRO will monitor and report operational risk events that impact customers, thus potentially becoming conduct risk events. These events will also be reported to ARCo, the senior management team and, where appropriate, to the ManCo and the President.

The Branch's Conduct Risk Framework focuses on the management of business areas and support functions, requiring the undertaking of periodic reviews by the Business of the conduct risks arising in the Branch from the activities performed and reporting those risks to senior management, ensuring that clear policies and procedures are in place to mitigate those risks and ensuring that all staff receive training in those policies and procedures and in the general standards of conduct expected of Branch staff.

It also provides background and insight into the process to:

- Identify the conduct risks inherent in the business;
- Setting out who is responsible for managing the conduct of the business;
- Support mechanisms in place to enable staff to improve the conduct of the business and function;
- The escalation process in place for ManCo and senior management to gain oversight of the conduct of the organisation; and
- The identification of bottlenecks or incentives to undermine the strategy to manage conduct risks.

**The Five Questions for Conduct Risk for Wholesale Banks**

The FCA has published five questions, consideration of which is expected by all wholesale banks in dealing with conduct risk and the risk management thereof. In the following CNCBLB sets out answers to these five questions:

**Question 1:** What proactive steps does the firm take to identify the conduct risks inherent within its business?

- The Branch considers conduct risk to comprise a range of different risks all and will manage these in accordance with the Conduct Risk Policy Framework. The Conduct Risk Policy Framework makes up part of the overarching RMF and, together with the Customer Journeys drawn up for each core product category and the associated Conduct Risk assessments,

informs the Risk Matrix which captures the universe of risks identified as inherent to the business planned by the Branch;

- The Conduct Risk Policy Framework brings together the suite of policies being implemented in the Branch to ensure individual conduct risks are understood and managed day-to-day;
- By assessing conduct risk based on Customer Journeys and in accordance with the Risk Scoring Methodology as set out in the RMF, while ensuring all staff operate in accordance with the Conduct Risk Policy Framework, CNCBLB is able to ensure conduct risk is identified across the product set regardless of the means of distribution;
- In addition, the Compliance department will be implementing the Compliance Monitoring Plan ("CMP") which ensures a range of monitoring activities across the range of compliance risks are carried out on a periodic basis. The CMP is directly informed by the Risk Matrix and the risk scoring of individual risks (i.e. the 'net' risk associated with each compliance risk including conduct risk) and therefore ensures a clear link exists between identification of conduct risk, the understanding of its severity and the monitoring of its mitigation though adherence to the suite of conduct risk related policy being put in place (see the Conduct Risk Policy Framework for a list of conduct risk related policies); and
- Training will be provided to all staff as part of their induction and on a periodic basis to ensure clarity as to what constitutes conduct risk and how it arises in respect of individual roles within the Branch.

**Question 2:** How does the firm encourage the individuals who work in front, middle, back office, control and support departments to feel responsible for managing the conduct of their business?

- The RMF clearly sets out both the range of risks inherent in the planned Branch business as well as the ownership 'allocation'. A core principle of the RMF is that the first line is the primary risk owner for all risk types with the second line providing oversight and framework within which the first line must operate;
- This principle and the associated expectations to individuals taking responsibility for risk management in their role will form part of training and be a principle role-modelled by the management team;
- To align day-to-day operation and behaviours to this principle the performance management process will be based on a balanced scorecard approach expressly taking account of peoples' adherence to conduct risk policies and demonstration of conduct risk awareness day-to-day; and
- Furthermore, while all staff will have the ability to earn discretionary bonuses linked to performance, these incentive schemes will not be solely driven by P&L contribution or business volumes generated. Instead, high performance will be linked back to the balanced scorecard

and non-compliance with policies will form part of year end compensation discussions with deliberate and/or persistent non-compliance directly affecting negatively the ability of staff to earn bonuses and / or pay rises.

**Question 3:** What support mechanisms do you have to enable people to improve the conduct of their business or department?

- In addition to the implementation of the Conduct Risk Policy Framework, the periodic compliance monitoring, staff training and the overarching performance management approach, the CCO and the wider compliance team will be expected to remain abreast of both regulatory expectations and industry practices in respect of conduct risk (and any other compliance risk);
- This will be achieved through participation in industry fora such as the UK Chinese Bankers Association; the Association of Foreign Banks; and attendance at briefings and roundtables hosted by professional services firms from time to time;
- Once the CCO has been appointed the allocation of individual roles across the Compliance department will be finalised. This will likely include the appointment of one or two 'Conduct Risk Champions' to work closely with the first line to ensure conduct risk is identified and managed appropriately throughout the Branch; and
- Furthermore, it is envisaged that the IA Plan will periodically include consider conduct risk and its management within the Branch. As a third party will be appointed to perform the IA department on an outsourced basis the expectation is that recommendations by this third party based on industry insight will also enable improvements where necessary across the Branch.

**Question 4:** How the committees gain oversight of the conduct of the organisation and consider conduct in their deliberations?

- The ARCo is tasked with oversight and challenge across the Risk agenda including specifically in respect of compliance risks and the content of the CMP as well as relevant policies and framework documents (e.g. the RMF and the Conduct Risk Policy Framework);
- ManCo through exercising the delegated authority from the President, must review and approve all policies as well as the CMP and the framework documents, at least annually;
- This provides both committees with line of sight and direct ability to influence the Branch's approach to conduct risk management from a framework 'design'; and
- In addition, MI will be in place and provided to both committees on a periodic basis showing how the Branch is performing in terms of conduct risk relative to RAS. It is anticipated that the MI suite will be finalised as one of the key priorities following appointment of the CCO.

**Question 5:** Has the firm assessed whether there are any other activities that it undertakes/ways in which it operates that could undermine strategies in place to improve conduct?

- The risk assessment process based on the RMF and the associated risk scoring methodology informs the view of inherent conduct risk within the Branch (which is reflected in the Risk Matrix and the CMF);
- It should be noted that even unregulated activities such as Spot FX, are also captured in the risk assessment and therefore CMP;
- CNCBLB believes that this process ensures conduct risk is fully understood and appropriately managed; and
- The fact that the Risk Matrix and CMP are reviewed at least annually, and that the Compliance Department is tasked with ensuring the Branch remains informed of industry practice (including the action taken by peer banks following instances of crystallised conduct risk), will ensure that any activities potentially undermining the wider conduct risk management arrangements are appropriately identified to ensure controls can be put in place.

### 7.5 Liquidity Risk

Liquidity risk is the risk that the Branch does not have sufficient liquidity resources available to enable to it meets its payment obligations as they fall due. Liquidity risk can also take form if the Branch is unable to obtain adequate funding in a timely manner at a reasonable cost.

The Branch is expected by HO to develop and maintain appropriate liquidity policies and limits to ensure prudent day to day operations.

ALCo will support ManCo in ensuring ongoing adherence to the limits set for liquidity risk.

The Branch has identified two material sources of liquidity risk detailed below:

- **Asset liquidity risk***:* Asset that are not repaid as per the contractual agreement and therefore are not fully recovered on schedule will impact the Branches cashflow. The non-receipt of cash in-flow could impact repayment of maturing liabilities and any new loans or other planned or contractual financing needs; and
- **Liability liquidity risk***:* Deposit funds, especially funds raised by the Branch, fluctuate irregularly due to changes in the internal and external factors, which triggers shocks and the relevant risk of loss of external funding. The change in the bank's ability to raise funding may affect the original financing arrangements, forcing the Branch to make adjustments in asset and liability management, causing increased liquidity risk. Under such circumstances, the bank may

be forced to liquidate positions/financing early, making the potential losses on the books turn into the actual losses and even causing bankruptcy.

### 7.6 Compliance & Regulatory Risk

In terms of compliance risk, the risk is caused by failing to adhere to policies, procedures and framework as mandated by regulatory, risk and business requirements. The Branch is aware that as part of its day to day operations it will open itself to many different forms of compliance risk such as:

***Regulatory Risk***

The Branch defines regulatory risk as the failure to meet UK or Chinese regulatory requirements.

The risk is defined as the impact of changes in any regulatory rule which could include Prudential requirements, Anti-Money Laundering / Counter-Terrorism Financing, transaction reporting, insider dealing and failing to prevent market manipulation by Branch staff. The Branch accords the highest importance to complying with applicable banking regulation at all times and has no appetite for any breach in regulatory rules or requirements.

From a conduct perspective, The Branch will only offer its customers “plain vanilla” services and products, and will ensure that its staff training and documented processes and procedures, are of sufficient standard to minimise the risk of compliance failures or reputational issues arising from its dealings with customers.

***Managing Conflicts of Interest***

As a financial services firm operating in the UK, the Branch is potentially exposed to conflicts of interest in its various activities, including potential conflicts with HO and its departments, which must be managed appropriately.

The Branch considers conflicts of interest under the general banner of conduct risk and the general approach to managing such a risk. In line with the Branch’s zero tolerance for conduct risks, it ensures that all practical steps are taken to identify, monitor and mitigate conflicts of interest as they arise in the course of business.

Conflicts of interest may arise in all areas of the Branch’s business and corporate activities. As for conduct risk generally, the Branch manages its conflicts by establishing a clear framework of policies and procedures for identifying, assessing and managing conflicts which may cause a material risk of damage to its customers’ interests, to the interests of the Bank or other parts of the

CITIC Group, to the Branch's reputation or its ability to meet regulatory requirements, and by providing appropriate training for all staff in these policies and procedures. The 1LOD for managing conflicts of interest are the departments and supporting functions in which they arise.

In order to manage conflicts of interest effectively, each department is required to:

- Ensure that conflicts of interest are taken into account in all business decisions;
- Identify the potential conflicts of interest in their respective business area. These may include situations where Branch staff:
    - Could arrange for the Branch to make a financial gain, or avoid a financial loss, at the expense of a third-party;
    - Have an interest in the outcome of a service provided to a third-party or of a transaction carried out on behalf of the third-party, which is inconsistent with that third-party's interest in the outcome;
    - Have a financial or other incentive to favour the interest of another party over the interests of a third-party;
    - Carry on the same or similar business as a third-party;
    - Receive or will receive from a third-party, or another party, a financial or other inducement in relation to a service provided, other than the standard commission or fee for that service; and
    - Receive information that could benefit them at the expense of either the firm or the third-party.
- Identify actions to mitigate these conflicts of interest and enact policies and procedures to implement those actions – this may involve the Branch changing the way it organises its business, including governance arrangements;
- Communicate these conflicts of interests and mitigating actions to the Compliance Department and where appropriate the corresponding HO departments;
- Ensure that all staff are familiar with the policies and procedures around conflicts of interest and have regular training in them; and
- Ensure that staff incentives and performance management promote the identification and management of conflicts of interest.

Under the Branch's Conflicts of Interest Policy, the Compliance Department carries out the following on a regular basis:

- Documents the Conflicts Matrix with the conflicts of interest identified and communicated to it by the departments and supporting functions, and mitigating actions;
- Challenges the departments and supporting functions to ensure all conflicts of interest are identified and that the potential conflicts arising in business decisions have been fully considered;
- Identifies the key conflicts of interest and regularly reports these to ARCo, senior management, ManCo, the President and HO where appropriate;
- Carry out appropriate Root Cause Analysis to identify trends and reasons for conflicts of interest occurrences and provide strategy to manage these going forward;
- Develop training materials for staff on conflicts of interest identification and mitigation and ensure adherence to them; and
- Ensure staff remuneration, incentives and performance management reflect the policies around conflicts of interest management.

The Branch relies on services provided by HO in carrying out and managing its businesses. This gives rise to potential conflicts of interest, including:

- One entity undertaking activities which are not in the interests of the other entity or their customers;
- Individuals conducting business on behalf of one entity in a way which disadvantages the other entity;
- Individuals focusing undue time and effort on behalf of one entity, to the disadvantage of the other entity;
- Individuals having access to confidential customer information that may benefit one entity over the other; and
- Remuneration and other incentive arrangements encouraging staff to benefit one entity over another.

These conflicts of interest are mitigated by:

- Developing clear and consistent policies and procedures, and ensuring they are implemented fully;
- Providing regular staff training in those policies and procedures;
- Developing and ensuring clear controls, policies and procedures around managing information flows between entities; and
- Recording of these potential conflicts of interest in the Branch's Conflicts Matrix and reviewing of this regularly with both the Branch's and the Bank's senior management.

***Treating Customers Fairly***

In order to minimise the occurrence of conduct risk the Branch will put the interests of its customers at the heart of the business. The culture of the Bank supports the concepts of Treating Customers Fairly ("TCF"), and the Branch will ensure the fair treatment of its customers by embedding the cultural values of the Bank and by adopting UK best practice in its interactions with customers, supported by a fair and transparent complaints procedure (see the TCF Policy and the Complaints Handling Policy).

The Branch will ensure that:

- Dealings with customers whether verbally or in writing always demonstrates the highest standard of personal and corporate integrity and unwavering courtesy, clarity and professionalism;
- The customer understands the nature of the products or services which we provide to them and any risk involved and all information provided is clear, fair and not misleading;
- The customer understands the amount and the nature of any actual and/or contingent obligations and liabilities (including any fees or charges) both at the outset and throughout the life of the product;
- The customer always knows who they can contact within the Branch if they have a question or wish to discuss, or complain about any of our products or services;
- All staff, including local and expatriate hires, will undergo compulsory induction and ongoing annual training outlining their obligations under the Branch's TCF policy, including role specific training on the COCON rules; and
- Performance management takes into consideration employee adherence to the Branch's corporate vales and the Individual COCON rules, which will include elements of goal setting and measurable achievements against these conduct related metrics.

***Complaints Handling***

In order to ensure that the Branch is able to continually improve its customer experience and rectify any circumstances which may mean it is not able to deliver on its commitment to TCF, it will establish a complaints procedure to record instances where customers have been unsatisfied with the product or service provided by the Branch.

Although the Branch will not deal with 'eligible complainants' as defined in Dispute Resolution: Complaints ("DISP") 2.7 given the entirely wholesale nature of its business, the Branch has decided

to adopt a complaints procedure which is in line with the DISP rules and the FCA's expectations, including the following steps:

- The logging and categorisation of complains on a Complaints Register;
- Acknowledging the complaint within five days of it being made where it cannot be resolved within three business days;
- Sending out a standardised Summary Resolution Communication where a complaint is resolved to the customer's satisfaction within three business days;
- Investigating complaints and keeping customers informed if an investigation is expected to take more than two weeks;
- Providing an update or a final response within eight weeks of receipt of the complaint;
- Ensuring that a full complaint resolution only takes more than eight weeks in exceptional circumstances; and
- Ensuring the Branch follows through promptly with any offer of remedial action and/or redress.

By adopting this approach, the Branch is demonstrating its willingness to adopt UK regulatory best practice, and ensure a consistent approach to dealing and managing complaints and resolving any disputes to the customer's satisfaction.

This standard procedure will also help the Branch collate valuable MI to ensure the Branch is able to:

- Improve areas of relevant areas of the business and its interactions with customers;
- Understand the performance of a particular product or service;
- Identify potential or crystallised areas of conduct risk and their root cause;
- Continue to apply TCF principles to its customers; and
- Effectively manage areas of the business / individuals which may be underperforming in relation to TCF principles.

For further information please refer to the Branch Complaints Handling Policy.
The Branch will look to resolve any disputes that a customer may have by providing an independent (internal) review from an ably competent second line individual assess the disputed case. This will be quality assured by the CCO. If resolution cannot be agreed on the back of the 2nd line review then either settlement will be considered or legal dispute resolution may be considered, dependant on the nature and scale of the case.

**Fraud Risk**

Fraud risk can affect the Bank through either internal or external factors. The Bank expects all employees to be aware of the risk of fraud and to report fraud, actual or potential, as well as where operating procedures etc. are insufficient and where the insufficiency could result in a fraud.

It is the responsibility of the individual managers of each of the various business areas to be aware of potential fraud and to ensure that controls are in place to limit the possibility of a fraud.

The Fraud Policy is maintained by Compliance department and sets out the Bank's Policy on the reporting and investigation of a fraud.

***Compliance Management Information***

CITIC Bank is cognisant of the importance of having appropriate MI to understand and identify trends arising in both the risk profile of the Branch as well as its financial performance. Planned MI will therefore cover a range of areas including Conduct Risk and TCF.

Specifically, in the context of conduct risk, the Branch will ensure appropriate MI is reviewed by the ARCo on a monthly basis. Where MI suggests the existence of, or a possibility of a detrimental outcome for its customer, the ARCo will be responsible for further analysis by the appropriate department, and/or a remediation plan is put in place to ensure any failings are understood and addressed. TCF MI will be reported to the ManCo on a quarterly basis, alongside any remedial work and actions agreed by the ARCo.

### 7.7 Legal Risk

Legal risk is the risk of loss caused by a transaction failing to perform in the way expected due to failure to correctly document, enforce or adhere to contractual arrangements, or due to the legal process failing to enforce the terms of a contractual arrangement or due to a change in the law.

Note that the risks associated with legal actions arising from the Branch's activities are considered to be operational risks associated with those activities. The Branch identifies two key sources of legal risk in its business:

- **Lack of documentation or legally ineffective documentation**: transacting with counterparties prior to completing documentation or executing on the basis of ineffective documentation; and
- **Reliance on enforcement of netting and collateral agreements or guarantees:** evaluating credit exposures on the assumption that: (a) netting arrangements within the trade

documentation; and/or (b) collateral agreements and/or (c) guarantees will be enforceable, or will apply, in the event of a counterparty default.

The Branch will manage its legal and compliance risk by:

- Requiring approval from Risk Management Department before trading with a counterparty without agreeing documentation;
- Ensuring all documentation is independently reviewed by the Compliance Department; the Branch will seek the services of a reputable and experienced legal firm to supplement expertise and resource where appropriate.
- Obtaining external legal opinions on the applicability of netting agreements, collateral agreements and guarantees where appropriate, in all relevant legal jurisdictions;
- Reviewing the assumptions used in credit risk exposure methodology for netting and the ability to take account of collateral and guarantees;
- Ensuring that any obligations arising from documentation affecting the Branch are communicated to the relevant departments;
- Ensuring all policies and procedures are adhered to as per compliance requirements;
- Carry out periodic monitoring to test if breaches are occurring. If so, Compliance will carry out Root Cause Analysis to identify themes to allow remedial action to be taken;
- Ensure staff have carried out mandatory compliance training; and
- The Compliance department will monitor the activity of the Branch, together with any additional investigations as deemed necessary to provide regular compliance oversight of the Branch and its activities.

## 8 Policies Approval Matrix

The major policies that form the overall governance and risk management framework are summarised below:

| Policy | Ownership responsible | Review | Approval | Head Office |
|---|---|---|---|---|
| **Ho Delegated Authority** | **President** | | | **CNCB Vice President** |
| **Risk Appetite Statement** | **CRO** | **President** | **ManCo** | **Aligned** |
| **Risk Management Framework** | **CRO** | **President** | | **Aligned** |
| **Senior Management Cover** | **HR** | **President** | | |
| **Credit Approval and Credit Risk Management Policy** | **CRO** | **CCo** | | **Aligned** |
| **Market Risk Policy** | | **ALCo** | | **Aligned** |
| **Liquidity Risk Policy** | | **ALCo** | | |
| **Operational Risk Policy** | | **Risk Department** | | |
| **Outsourcing Risk Policy** | | **Risk Department** | | |
| **Business Continuity Framework** | | **Risk Department** | | **Aligned** |
| **New Product Approval** | | **Risk Department** | | |
| **Conduct Risk Policy Framework** | | **Risk Department** | | |
| **Compliance Manual** | | | | |

| | | | | |
|---|---|---|---|---|
| **Prevention of AML/CTF Policy** | | | | **Aligned** |
| | | | | |
| **Conflicts Management Policy** | | | | **Aligned** |
| **Best Execution** | **CCO** | **ARCo** | **ManCo** | **Aligned** |
| **Fraud Policy** | | | | **Aligned** |
| **Anti-Bribery & Corruption Policy** | | | | **Aligned** |
| **Whistle Blowing Policy** | | | | **Aligned** |
| **IT Risk** | **Head of IT** | | **ManCo** | **Aligned** |
| **Information Security** | | | | **Aligned** |
| **Data Protection** | | | | **Aligned** |
| **Staff Handbook** | **HR** | | **ManCo** | |
| **Remuneration Policy** | | | | |

# 9 Appendix A – CNCBLB approved SMF's

| | Function | CNCBLB approved person | CNCBLB Title |
|---|---|---|---|
| SMF 19 | Head Overseas Branch | Jinlei Xu | President |
| SMF 22 | Other Local responsibility | Gang Zhao | Vice – President |
| SMF 22 | Other Local responsibility | Richard Thasis | Head of Financial Markets |
| SMF 22 | Other Local responsibility | Di Wang | Head of Information Technology |
| SMF 24 | Other Local responsibility | Anthony Chong | Head of Operations |
| SMF 2 | Chief Financial Officer | Colin Marshall | Head of Finance and Accounting |
| SMF 4 | Chief Risk Officer | Grant Lowe | Chief Risk Officer |
| SMF 16 | Compliance | Rhod Sutton | Chief Compliance Officer |
| SMF 17 | Money Laundering Officer | Rhod Sutton | Chief Compliance Officer |

## 10 Appendix B – Principles & Conduct rules

### FCA Principle of Business

| | | |
|---|---|---|
| 1 | Integrity | A firm must conduct its business with integrity. |
| 2 | Skill, care and diligence | A firm must conduct its business with due skill, care and diligence. |
| 3 | Management and control | A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. |
| 4 | Financial prudence | A firm must maintain adequate financial resources. |
| 5 | Market conduct | A firm must observe proper standards of market conduct. |
| 6 | Customers' interests | A firm must pay due regard to the interests of its customers and treat them fairly. |
| 7 | Communications with clients | A firm must pay due regard to the information needs of its clients, and communicate information to them in a way which is clear, fair and not misleading. |
| 8 | Conflicts of interest | A firm must manage conflicts of interest fairly, both between itself and its customers and between a customer and another client. |
| 9 | Customers: relationships of trust | A firm must take reasonable care to ensure the suitability of its advice and discretionary decisions for any customer who is entitled to rely upon its judgment. |
| 10 | Clients' assets | A firm must arrange adequate protection for clients' assets when it is responsible for them. |
| 11 | Relations with regulators | A firm must deal with its regulators in an open and cooperative way, and must disclose to the FCA appropriately anything relating to the firm of which that regulator would reasonably expect notice. |

FCA Conduct Rules

| **FIRST TIER: ALL STAFF (excluding auxiliary staff)** |
|---|
| 1. You must act with ***integrity*** |
| 2. You must act with ***due skill, care and diligence*** |
| 3. You must be open and cooperative with ***FCA, the PRA and other regulators*** |
| 4. You must pay due regard to the ***interests of customers*** and treat them fairly |
| 5. You must observe proper standards of ***market conduct*** |
| **SECOND TIER: REQUIREMENTS FOR SENIOR MANAGEMENT ONLY** |
| **SM1**<br>You must take reasonable steps to ensure that the business of the firm for which you are responsible is ***controlled*** effectively |
| **SM 2**<br>You must take reasonable steps to ensure that the business of the firm for which you are responsible ***complies*** with the relevant requirements and standards of the regulatory system |
| **SM 3**<br>You must take reasonable steps to ensure that any ***delegation*** of your responsibilities is to an appropriate person and that you oversee this effectively |
| **SM 4**<br>You must ***disclose*** appropriately any information of which the FCA or PRA would reasonably expect notice |

## 11 Appendix C – Terms of Reference: Management Committee

## 12 Appendix D – Terms of Reference: Asset & Liability Committee

## 13 Appendix E – Terms of Reference: Audit & Risk Committee

## 14 Appendix F – Terms of Reference: Credit Committee